FIG. 3 shows a process (300) for playing a file that has been downloaded from the content server (160) to a playback device (105, 110). The process starts with receiving a user request to play an audio file on the playback device (105, 110) (step 305). In response to the request, the software on the playback device (105, 110) calls a storage medium validation function (step 307) for the storage medium where the audio file is located. The validation function is part of the CRM library and attempts to verify the integrity of the content rights file stored on the target storage file system by calculating the secure hash value of the content rights file for the selected medium and comparing this calculated hash value with the stored value in the playback device's protected storage area. If the media validation function fails, the device will not play any files that are stored on the storage medium.

If the validation is successful, the process checks the record in the content rights file associated with the requested audio file to see if the audio file is time-limited (step 310). The time limitation associated with a file can either be an absolute time limitation such as "This file will no longer be valid after October 1, 2002," or relative time limitation such as "This file will be valid for 24 hours from the time it is first played on this the playback device." If there is a time limitation associated with the file, the process continues by checking whether the expiration time (relative or absolute) has passed (step 315). If the expiration time has passed, the process refuses to play the file until a new expiration time has been obtained from the content server (160) (step 320).

If the process determines that the expiration time has not passed (step 315), or if the file is not time-limited (step 310), the process continues by checking the content rights file to see if the file is limited to a certain number of playbacks (step 325). If the file is limited to a certain number of playbacks, the process checks if all playbacks have been used (step 330). If all the playbacks have been used, the process refuses to play the file until the file expiration information, that is, the maximum number of playbacks, has been refreshed (step 335). If there are still playbacks left (step 330), or if the file does not have any associated maximum number of playbacks (step 325), the process proceeds to play the audio files to the user and update the content rights file if necessary, for example, if a remaining playback count is decremented (step 340). When the content rights file is updated, the hash is recalculated and the hash value stored in the secure storage area is updated.

In one implementation, every time the user connects to the content server (160), using the communication module (120, 125) for a particular playback device (105, 110), the server generates the time stamp that is transferred to the communication module (120, 125) and subsequently to the playback device (105, 110). If an audio file is time-limited and the playback device (105, 110) does not have a secure clock, that is, the clock in the playback device (105, 110) can be manipulated by a user, the playback process uses the time stamp as a reference time when checking if the expiration time has passed (see step 315, in FIG. 2). The time stamp is also used as a reference if the playback device (105, 110) has no internal clock at all. This time stamp will not be as exact as a secure clock, but will work well since it is updated every time the user connects to the content server (160) and a user can be encouraged to connect to the server by additionally limiting the playback rights by allowing only a limited number of playbacks at a time.

FIG. 4 shows a process (400) for refreshing expiration information associated with one or more audio files residing on a user's playback device (105, 110). The process starts by receiving a request for refreshing expiration information associated with audio files (step 405). This request can be received from the user, for example through a web page hosted by a service provider on which the user can manage audio files associated with his or her playback device (105, 110) or account. Alternatively, the request can be generated automatically as part of the download process, such as the one shown in FIG. 2, or when a user tries to play back files using a jukebox application performing a process such as the one shown in FIG. 3. The process validates the content rights and rights associated with the device and the associated user account (step 410), in the same manner that was described above for step 215 (FIG. 2).

If the content rights, that is, the rights associated with a device and the user rights associated with the user account are validated, that is, if the user is allowed to transfer the audio files to his or her playback device (105, 110), the process continues by deciding whether the rights can be refreshed without any additional user action (step 415). The additional user action can, for example, involve paying more money in order to extend the expiration condition (play count or time period) or downloading a promotional file before extending the expiration for the desired audio file, and so on. If a user action is needed, the process prompts the user to perform the user action (step 420). The process then checks if the user has taken a necessary action (step 425). If the user has taken the action, or if the audio files can be refreshed without a user action (step 415), the process continues and transmits the refreshed rights to the communication module (120, 125) associated with a playback device (105, 110) (step 430). If the audio files still reside on the device but have expired, only the updated expiration information is sent to the communication module (120, 125). If the audio files have been deleted from the playback device (105, 110), the process also transfers the refreshed to audio files with their rights to communication module (120, 125) for the particular playback device (105, 110).

In one implementation, the content rights file on the playback device (105, 110) is updated by a content rights management module running on the content server (160) by appending a secure signed command block to the content rights file. The validation function, which was discussed above, verifies the command block signature and executes the command on behalf of the content server (160). As was described above, typical refreshing commands include reset CRM, set play count, set absolute expiration time, set relative expiration time, send a time stamp to the playback device (105, 110), and delete a record (that is, an audio file entry) from the content rights file. If the user does not take a necessary action in step 425, the process denies refreshing the rights associated with the audio file (step 435).

The invention can be implemented in digital electronic circuitry, or in computer hardware, firmware, software, or in combinations of them. Apparatus of the invention can be implemented in a computer program product tangibly embodied in a machine-readable storage device for execution by a programmable processor; and method steps of the invention can be performed by a programmable processor executing a program of instructions to perform functions of the invention by operating on input data and generating output. The invention can be implemented advantageously in one or more computer programs that are executable on a programmable system including at least one programmable processor coupled to receive data and instructions from, and to transmit data and instructions to, a data storage system, at least one input device, and at least one output device. Each computer program can be implemented in a high-level procedural or object-oriented programming language, or in assembly or machine language if desired; and in any case, the language can be a compiled or interpreted language. Suitable processors include, by way of example, both general and special purpose microprocessors. Generally, a processor will receive instructions